УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 151, кн. 2 Физико-математические науки *2009*

УДК 519.714

О СЛОЖНОСТИ ОДИН РАЗ ЧИТАЮЩИХ ВЕРОЯТНОСТНЫХ ПРОГРАММ

Р.Г. Мубаракзянов

Аннотация

Упорядоченные один раз читающие ветвящиеся программы представляют собой удобное средство описания логических схем, булевых функций. Вместе с тем не только детерминированные, но и вероятностные с ограничением на ошибку упорядоченные один раз читающие ветвящиеся программы имеют неприемлемо большой (экспоненциальный) размер для ряда известных функций. Для вероятностных один раз читающих ветвящихся программ экспоненциальные нижние оценки сложности известны лишь при очень сильных ограничениях. В данной статье эти ограничения частично снимаются за счет перехода к ветвящимся программам, определяемым графом порядка. Для этих вычислительных моделей удается доказать экспоненциальные нижние оценки сложности.

Ключевые слова: булева функция, бинарная ветвящаяся программа, класс сложности, нижняя оценка сложности вычислений.

1. Основные определения

Определение детерминированных ветвящихся программ хорошо известно [1]. Эта модель определяется ориентированным ациклическим графом, у которого каждая вершина, за исключением двух выходов (стоков), соответствует некоторой переменной и имеет две исходящие дуги, помеченные нулем и единицей. Для фиксированных значений переменных вычисление начинается в единственной начальной вершине, идет по дугам в соответствии со значениями переменных и возвращает значение, которым помечен выход. Если на каждом пути каждая переменная встречается не более одного раза, то программа называется один раз читающей (*BP1*). Кроме того, если переменные читаются в каком-то определенном порядке, то программа называется упорядоченной *BP1*, или *OBDD*.

Ветвящаяся программа называется *недетерминированной*, если в ней допускаются недетерминированные узлы, то есть узлы, из которых выходят две непомеченные дуги. При наличии в ветвящейся программе вероятностных узлов, для которых выходная дуга определяется с вероятностью $1/2$, ветвящаяся программа называется *вероятностной* [2]. Для ε, $0 \le \varepsilon < 1/2$, будем говорить, что вероятностная ветвящаяся программа B $(1-\varepsilon)$-*вычисляет* функцию h, если B выдает $h(x)$ с вероятностью не менее $1-\varepsilon$ для каждого входа x. Такое вычисление называется $(1-\varepsilon)$-вычислением, или вероятностным с ограничением на ошибку, равным ε. Так как в настоящей статье рассматриваются лишь такие вычисления, будем называть их просто вероятностными.

На вероятностные и детерминированные программы естественным образом распространяются понятия *BP1* и *OBDD*. Под *сложностью* (или размером) ветвящейся программы подразумевается количество ее детерминированных узлов. Под *сложностью* вычисления (или реализации) функции понимается минимальная сложность вычисляющей ее программы в соответствующем классе.

Пусть M – некоторый класс ветвящихся программ, например, $OBDD$, $BP1$ и т. д. Тогда класс булевых функций, вычислимых детерминированными (недетерминированными) программами полиномиального размера типа M, обозначим P-M (NP-M). Пусть BPP_ε-M – класс функций, $(1-\varepsilon)$-вычислимых вероятностными ветвящимися программами типа M полиномиального размера. Тогда BPP-$M = \bigcup\limits_{0\le\varepsilon<1/2} BPP_\varepsilon$-$M$. Отношения между классами сложности P, BPP, NP в контексте $OBDD$ хорошо изучены [3]. Например, известна экспоненциальная нижняя оценка сложности вероятностных $OBDD$ [4]. Доказано также, что функция «целочисленное умножение» ($MULT_n$) сложна для вероятностных $OBDD$ [5]. Функция $MULT_n$ определяется на переменных $x_0,\dots,x_{n-1},\ y_0,\dots,y_{n-1}$ как n-й бит произведения

$$(x_0\dots x_{n-1})\times(y_0\dots y_{n-1}).$$

Ранее нами была исследована следующая ограниченная модель $BP1$ [6].

Определение 1. $BP1$ P на n переменных X назовем $BP1$ с большой $OBDD$ частью (для краткости $BP1(OBDD)$), если существует подмножество $X'\subset X$ переменных мощности $O(\log_2 n)$ и значения d переменных из X' такие, что подпрограмма P после фиксирования значений переменных из X' равными d является $OBDD$ на $X\setminus X'$.

В [6] нам удалось получить высокие нижние оценки сложности вероятностных один раз читающих ветвящихся программ с большой $OBDD$ частью для различных функций, в частности и для функции $MULT_n$. Было доказано также, что

$$BPP\text{-}OBDD \subset BPP\text{-}BP1(OBDD) \subset BPP\text{-}BP1.$$

В настоящей статье рассматриваются ветвящиеся программы, определяемые графом порядка. Исследуется сложность реализации функций соответствующими ветвящимися программами.

2. Ветвящиеся программы, определяемые графом порядка

Высокие нижние оценки сложности относительно легко получать для $OBDD$ в силу того, что они представляют собой сильно ограниченный класс ветвящихся программ, обладающих рядом удобных для исследования свойств. В [7, 8] независимо было предложено расширение класса $OBDD$ за счет фиксирования не порядка чтения переменных, а графа чтения переменных.

Определение 2. Граф G, называемый графом чтения переменных, является один раз читающей ветвящейся программой, имеющей один сток, причем на каждом пути от корня к стоку читаются все переменные. Говорят, что $BP1$ B имеет граф чтения переменных G, если выполняется следующее. Для любого набора значений входных переменных $x_1,\dots,x_n$, если переменная x_i читается в B перед переменной x_j, то x_i читается в G перед переменной x_j (заметим, что путь вычисления в G определяется единственным образом).

Ветвящиеся программы, имеющие граф чтения переменных, в англоязычной литературе называются *graph-driven*, и для их обозначения используется префикс *gd*. Обозначим программу, определяемую графом чтения G, через G-$BP1$.

Граф чтения переменных G, называемый также графом порядка, задает порядок, в котором будут читаться переменные, если зафиксировать их значения. Для $OBDD$ таким графом будет «линейный» граф с n вершинами, в котором дуги,

выходящие из одной вершины, ведут в одну и ту же вершину. Любая детерминированная $BP1$ имеет граф чтения переменных. Если зафиксировать граф чтения переменных G и рассматривать лишь один раз читающие ветвящиеся программы, имеющие один и тот же граф чтения переменных G, то можно снова легко манипулировать ветвящимися программами, в частности проверять их эквивалентность.

При расширении возможностей ветвящихся программ (при переходе к недетерминированным или вероятностным программам) соответствие некоторому графу порядка представляется сильным ограничением. Для недетерминированных (вероятностных) $BP1$ граф чтения переменных не всегда определен, так как при одних и тех же значениях переменных они могут читаться в зависимости от недетерминированного (вероятностного) выбора в различном порядке. Тем не менее в силу сложности исследования таких классов возникает необходимость сужения даже класса gd-программ.

Определение 3. Недетерминированная один раз читающая ветвящаяся программа B, имеющая граф чтения переменных G, называется хорошо структурированной (well-structured), если существует отображение f множества вершин B на множество вершин G такое, что каждая вершина v в B и ее образ $f(v)$ в G помечены одной и той же переменной. Кроме того, для любого набора значений входных переменных $x_1, \ldots, x_n$: если вычисление в B проходит через вершину v, то вычисление в G проходит через вершину $f(v)$.

Это означает, что переход в хорошо структурированной программе не только соответствует G (как для gd-программ), но и определяется упомянутым отображением. Для gd-программы B вершина v, достижимая на различных наборах a и b, может соответствовать различным вершинам G. Дело в том, что хотя переменные, прочитанные в B до v, не могут встречаться после v, они могут читаться в разном порядке. В зависимости от недетерминированного (вероятностного) выбора программа с корнем B читает переменные в различном порядке. Но этот порядок должен однозначно определяться значениями прочитанных переменных.

Б. Боллиг получила результаты о соотношении классов сложности, образованных при рассмотрении недетерминированных $BP1$, имеющих в качестве графа чтения переменных дерево [9] (заметим, что класс $BP1(OBDD)$ является обобщением этих программ), и показала, что умножение сложно и для таких ветвящихся программ. Затем в соавторстве с другими исследователями [10, 11] результат был распространен на хорошо структурированные недетерминированные $BP1$.

3. Вероятностные ветвящиеся программы, определяемые графом порядка

Представляет интерес следующий факт:

Лемма 1. *Пусть B – вероятностная gd-$BP1$ от n переменных с графом чтения G, $(1-\varepsilon)$-вычисляющая функцию f для некоторого $\varepsilon \in [0, 1/2)$. Тогда существует хорошо структурированная вероятностная G-$BP1$ R, в которой вероятностные вершины расположены до чтения любой детерминированной переменной, $(1-\varepsilon')$-вычисляющая функцию f для произвольного $\varepsilon' \in [\varepsilon, 1/2)$. При этом размеры (количество вершин) программ связаны неравенством $|R| \leq \leq O(n)|B|$.*

Доказательство. Пусть максимальное число вероятностных вершин в B на пути до финальной вершины равно m. Тогда существует множество выборов вероятностных переходов $\{a_1, a_2, \ldots a_t\}, t \leq 2^m$, каждый из которых фиксирует детерминированную G-$BP1$ на детерминированных переменных. Обозначим множество соответствующих G-$BP1$ через $Q = \{B_1, B_2, \ldots B_t\}$, $t \leq 2^m$.

Для произвольного r выберем случайным образом независимо r программ из множества Q и построим вероятностную G-$BP1$ R так, что в начале программы расположены вероятностные узлы, образующие дерево, листья которого соответствуют корням выбранных программ. Для фиксированного набора значений переменных $\{x_1, x_2, \dots x_n\} = y$ обозначим через $P_R(y)$ вероятность того, что полученная программа R дает неверное значение функции f на y. Пусть $P(y)$ – вероятность того, что $P_R(y)$ для случайно выбранной программы R больше $\varepsilon' \in [\varepsilon, 1/2)$. Известно [12], что $P(y)$ не превышает $c(\varepsilon, \varepsilon')^r$ для некоторого фиксированного $c(\varepsilon, \varepsilon') < 1$. Пусть $r > n \log_{c(\varepsilon,\varepsilon')}(1/2)$. Тогда $P(y) < (1/2)^n$.

Представим себе прямоугольник, разбитый на вертикальные и горизонтальные полосы одинаковой ширины. Вертикальные полосы соответствуют всевозможным значениям переменных функции f (их количество равно 2^n), а горизонтальные полосы – всевозможным программам R. Заштрихуем пересечение полос, для которых $P_R(y)$ больше ε'. Заштрихованной может быть менее $(1/2)^n$ площади любого столбца. Следовательно, найдется горизонтальная полоса без заштрихованных элементов. Она соответствует искомой программе R. Для размеров программ верно неравенство $|R| \le r|B|$. Так как r можно взять равным $\lfloor n \log_{c(\varepsilon),\varepsilon')}(1/2) \rfloor$, то $|R| \le O(n)|B|$.

По построению программу R можно разделить на две части. В корневой части располагаются вероятностные вершины и они образуют дерево. Каждый лист этого дерева порождает подграф, являющийся детерминированной G-$BP1$. Сохраняя приведенные оценки размера R, можно построить программу так, чтобы эти подграфы не пересекались. Тогда свойство хорошей структурированности для R выполнится. □

Для произвольной хорошо структурированной вероятностной $BP1$ верно следующее.

Лемма 2. *Пусть B – хорошо структурированная вероятностная G'-$BP1$ от n переменных. Тогда существует граф G, являющийся графом порядка, такой, что B является хорошо структурированной вероятностной G-$BP1$. При этом размеры (количество вершин) программ связаны неравенством $|G| \le 2(n-1)|B|$.*

Доказательство. Удалим из G' вершины, для которых отсутствуют в B вершины, соответствующие функции хорошей структурированности. Если дуга ведет в удаляемую вершину v, перенаправим ее в любой неудаляемый потомок w вершины v. Свойство хорошей структурированности позволяет однозначно восстановить w. В результате размер полученного из G' графа не более чем $|B|$. Поскольку в графе порядка на каждом пути от корня до стока читаются все переменные, необходимо добавить между вершинами v и w для каждой дуги (v, w) фиктивные вершины с пометками тех переменных, которые не прочитаны на путях от корня до v, но могут быть прочитаны на путях от корня до w. Так как из каждой вершины выходит 2 дуги, которые могут вести в $OBDD$ длины не более чем $n-1$, получаем требуемую оценку . □

Из доказанных лемм вытекает

Следствие 1. *Пусть B – вероятностная gd-$BP1$ от n переменных с графом чтения G, $(1-\varepsilon)$-вычисляющая функцию f для некоторого $\varepsilon \in [0, 1/2)$. Тогда существует граф чтения G и хорошо структурированная вероятностная G'-$BP1$ R, в которой вероятностные вершины расположены до чтения любой детерминированной переменной, $(1-\varepsilon')$-вычисляющая функцию f для произвольного $\varepsilon' \in [\varepsilon, 1/2)$. При этом размеры (количество вершин) программ связаны неравенством $|G'| \le O(n^2)|B|$.*

Теорема 1. *Функция $MULT_n$ от $2n$ переменных $Z = X \cup Y$ экспоненциально сложна для вероятностных один раз читающих ветвящихся программ, имеющих граф чтения.*

Доказательство. Доказательство теоремы практически полностью совпадает с доказательством для недетерминированного случая [10]. Детали этого доказательства довольно сложны, поэтому рассмотрим лишь основные идеи.

Рассматривается подфункция $MULT_n^*$ функции $MULT_n$, осуществляющая перемножение лишь нечетных чисел ($x_{n-1} = y_{n-1} = 1$). Рассмотрим множества A, B, Y двоичных целых чисел, имеющих не более чем n разрядов, причем Y содержит лишь нечетные числа. Построим матрицу M следующим образом. Для произвольных чисел $a \in A$, $b \in B$, $y \in Y$ элемент матрицы M на пересечении строки, соответствующей a, и столбца, соответствующего (b, y), равен $MULT_n^*(a + b, y)$. В [10] доказано, что M содержит треугольную подматрицу, нижняя оценка для размера s которой определяется соотношениями, зависящими от мощностей множеств A, B, Y. Для получения этих соотношений строятся такие подмножества $\{a_1, \ldots, a_s\} \subseteq A$, $\{b_1, \ldots, b_{s-1}\} \subseteq B$ и число $y \in Y$, что

$$MULT_n^*(a_i + b_j, y) = 1 \Leftrightarrow i < j.$$

Данный поиск далеко не тривиален и не сводится (как в случае более простых моделей) к рассмотрению чисел y, содержащих две единицы, когда умножение фактически является сложением «частей» первого сомножителя, и, соответственно, необходимо определить, осуществляется ли при сложении «перенос» разряда или нет. Заметим, что для оценки s не важно, каковы множества A, B, Y, существенны лишь их мощности.

Пусть f – некоторая функция от n переменных X, а (X_1, X_2) – разбиение X. Рассмотрим некоторую функцию f_1 от переменных X. Пусть для любого вектора x_2 значений переменных из X_2 множество векторов x_1 значений переменных из X_1 таких, что на (x_1, x_2) функции f и f_1 совпадают, имеет мощность не менее чем $\varepsilon 2^{|X_1|}$. Тогда f_1 называется функцией, ε-близкой к f. *Фильтром* F множества X назовем определенное множество подмножеств X (см. [10]). Ассоциируя любое из этих подмножеств с X_2, получаем (X_1, X_2)-разбиение X, $X_1 = X \setminus X_2$.

Пусть F – фильтр множества X, и для любого ассоциированного с F (X_1, X_2)-разбиения X верно следующее. Для любой функции f', ε-близкой к f, сложность коммуникационного вероятностного (X_1, X_2)-протокола (вычислители читают переменные из X_1 и X_2 соответственно) не менее чем l. Тогда либо сложность вероятностной G-$BP1$ B, вычисляющей f, не менее чем $2^l + 1$, либо размер G более чем $1/\varepsilon$.

Доказательство ведется от противного, то есть размеры B и G ограничиваются сверху. В G любое ребро разбивает множество переменных X на подмножества: X_1 – тех переменных, которые прочитаны до этого ребра, и X_2 – оставшихся. Найдется ребро e, количество путей до которого не менее чем $2^{|X_1|}/|G|$. Рассмотрим следующее коммуникационное вычисление функции f', когда вычислители читают переменные из X_1 и X_2 соответственно. Первый вычислитель запускает B на путях до e и передает пометку вершины B второму вычислителю, то есть не более чем $\log_2 |B|$ бит. Второй вычислитель продолжает вычисление на B, начиная с полученной вершины. На других входах значение вычисляемой функции несущественно. Вычисляемая функция будет ε-близкой к f, и ее коммуникационная сложность будет меньше l. Получаем противоречие.

Для $MULT_n^*$ множество переменных разбито на X и Y. Фиксируются числа ε и k, зависящие от n, и фильтр F, содержащий подмножества мощности k.

Для любой ε-близкой к $MULT_n^*$ функции f верно следующее. Ассоциированное с F разбиение соответствует коммуникационному вычислению, когда первый вычислитель читает переменные из X_1, Y_1, а второй – из X_2, Y_2. Из теоретико-множественных соображений можно зафиксировать значения переменных из Y_1 так, что количество возможных значений переменных из X_1, на которых функции $MULT_n^*$ и f равны, не менее чем $\varepsilon 2^{k/2}$. Получаем коммуникационную матрицу, строки которой соответствуют данным значениям X_1, а столбцы – всевозможным значениям X_2, Y_2. Подобрав нужные значения ε и k, можно получить экспоненциальную нижнюю оценку на размер s треугольной подматрицы.

Как известно [5], предположение о полиномиальной вероятностной вычислимости функции g, имеющей большую треугольную подматрицу, приводит к выводу о полиномиальной вероятностной коммуникационной вычислимости любой функции f. Действительно, для такого коммуникационного вычисления первый вычислитель запускает вычисление g необходимое число раз на наборе x_1 своих переменных, второй вычислитель продолжает вычисление g, делая различные предположения о значениях x_1 и отождествляя их со значениями своих переменных. В зависимости от результатов он сможет определить правильно значение x_1 с необходимой вероятностью.

Так как размер s подматрицы экспоненциален и существуют функции, имеющие вероятностную коммуникационную сложность большую, чем логарифм от количества переменных, то получаем противоречие с предположением о полиномиальной вычислимости $MULT_n$ на вероятностных один раз читающих ветвящихся программах, имеющих граф чтения. □

Summary

R.G. Mubarakzjanov. On the Complexity of Randomized Read-once Branching Programs.

Ordered binary decision diagrams are a well known computational model. Graph-driven read-once branching programs presented in this paper generalize this model. Exponential lower bound of the complexity of such programs for integer multiplication is proven.

Key words: Boolean function, binary branching program, complexity class, computation complexity lower bound.

Литература

1. *Wegener I.* Branching Programs and Binary Decision Diagrams: Theory and Applications. SIAM Monographs on Discrete Mathematics and Applications. – Philadelphia, USA: Soc. Ind. Appl. Math., 2000. – 408 p.

2. *Ablayev F., Karpinski M.* On the power of randomized ordered branching programs // Proc. ICALP'96. LNCS. – Springer, 1996. – No 1099. – P. 348–356.

3. *Ablayev F., Karpinski M., Mubarakzjanov R.* On BPP versus $NP \cup coNP$ for Ordered Read-Once Branching Programs // Theoret. Comp. Sci. – 2001. – V. 264. – P. 127–137.

4. *Ablayev F.* Randomization and nondeterminism are incomparable for ordered read-once branching programs // Proc. ICALP'97. LNCS. – Springer, 1997. – No 1256. – – P. 195–202.

5. *Ablayev F., Karpinski M.* A lower bound for integer multiplication on randomized read-once branching programs // Electronical Colloquium on Computational Complexity: ECCC TR98-011. – Trier: Trier University, 1998. – URL: http://www.eccc.uni-trier.de/ECCC/.

6. *Мубаракзянов Р.Г.* Нижние оценки сложности вероятностных бинарных программ с большой упорядоченной частью // Изв. вузов. Матем. – 2006. – № 6. – С. 86–94.

7. *Gergov J., Meinel C.* Efficient Boolean manipulation with $OBDD$s can be extended to $FBDD$s // IEEE Trans. on Computers. – 1994. – No 43. – P. 1197–1209.

8. *Sieling D., Wegener I.* Graph driven BDDs – a new data structure for Boolean functions // Theoret. Comp. Sci. – 1995.– No 141. – P. 283–310.

9. *Bollig B.* Restricted nondeterministic read-once branching programs and an exponential lower bound for integer multiplication // RAIRO Theoretical Informatics and Applications. – 2001. – No 35. – P. 149–162.

10. *Bollig B., Woelfel Ph.* A lower bound technique for nondeterministic graph-driven read-once branching programs and its applications // Proc. of MFCS. LNCS. – Springer, 2002. – No 2420. – P. 131–142.

11. *Bollig B., Waack S., Woelfel Ph.* Parity graph-driven read-once branching programs and an exponential lower bound for integer multiplication // Proc. of IFIP 2nd Int. Conf. on Theoretical Computer Science. – 2002. – P. 83–94.

12. *Chernoff H.* A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations // Ann. Math. Stat. – 1952. – No 23. – P. 493–509.

Поступила в редакцию
16.03.09

Мубаракзянов Рустам Гамирович – кандидат физико-математических наук, доцент кафедры теоретической кибернетики Казанского государственного университета.

E-mail: *rustam@ksu.ru*